PROPOSED AMENDMENTS RELATING TO PAYMENTS ISSUES

CONTENTS

SECTION 3–104. NEGOTIABLE INSTRUMENT.

(a) Except as provided in subsections (c) and (d), "negotiable instrument" means an unconditional promise or order to pay a fixed amount of money, with or without interest or other charges described in the promise or order, if it:

(1) is payable to bearer or to order at the time it is issued or first comes into possession of a holder;

(2) is payable on demand or at a definite time; and

(3) does not state any other undertaking or instruction by the person promising or ordering payment to do any act in addition to the payment of money, but the promise or order may contain (i) an undertaking or power to give, maintain, or protect collateral to secure payment, (ii) an authorization or power to the holder to confess judgment or realize on or dispose of collateral, ~~or~~ (iii) a waiver of the benefit of any law intended for the advantage or protection of an obligor; (iv) an agreement as to what law governs the instrument; or (v) an undertaking to resolve a dispute concerning the promise or order in a specified forum.

SECTION 3–105. ISSUE OF INSTRUMENT.

(a) "Issue" means:

(1) the first delivery of an instrument by the maker or drawer, whether to a holder or nonholder, for the purpose of giving rights on the instrument to any person; or

(2) if agreed by the payee, first transmission by the drawer to the payee of an image of an item and of information derived from the item in a manner that enables the depositary bank to collect the item by transferring or presenting an electronic check under federal law.

(b) An unissued instrument, or an unissued incomplete instrument that is completed, is binding on the maker or drawer, but nonissuance is a defense. An instrument that is conditionally issued or is issued for a special purpose is binding on the maker or drawer, but failure of the condition or special purpose to be fulfilled is a defense.

(c) "Issuer" applies to issued and unissued instruments and means a maker or drawer of an instrument.

Official Comment

1. Under former Section 3–102(1)(a) "issue" was defined as the first delivery to a "holder or a remitter" but the term "remitter" was neither defined nor otherwise used. In revised Article 3, Section 3–105(a) defines "issue" more broadly to include the first delivery to anyone by the drawer or maker for the purpose of giving rights to anyone on the instrument. "Delivery" with respect to instruments is defined in ~~Section 1–201(14)~~ Section 1-201(b)(15) as meaning "voluntary transfer of possession."

Subsection (a) permits an instrument to be issued by an electronic transmission of an image of and information derived from the instrument by maker and drawer, rather than by delivery. Thus, for example, a drawer might, with the permission of the payee, write and sign a check, take a photograph of the check, send the photograph to the drawee for processing electronically, and destroy the original check. If the electronic image and the information derived from it can be processed as an "electronic check" under Regulation CC, see 12 C.F.R. § 229.2(ggg), the check is "issued" and hence can be enforced pursuant to this Article.

* * *

Reporter's Note

The phrase "transmission of an image of an item or information describing the item is derived from Section 4–110(a), dealing with electronic presentment.

SECTION 3–309. ENFORCEMENT OF LOST, DESTROYED, OR STOLEN INSTRUMENT.

* * *

Official Comment

* * *

4. The destruction of a check in connection with a truncation process in which information is extracted from the check and an image of the check is made, and then such information and image are transmitted for payment does not, by itself, prevent application of this section. See Section 3-604 comment 1.

Example: The payee of a check creates an image of the check, destroys the check, and transmits the image and information derived from the check for payment. Due to an error in transmission, the depositary bank never receives the transmission. The payee may be able to enforce the check if the payee can prove the terms of the check and otherwise satisfy the requirements of this section. The result would be different if there were no error in the transmission and the payor discharged its obligation on the check.

SECTION 3–604. DISCHARGE BY CANCELLATION OR RENUNCIATION.

(a) A person entitled to enforce an instrument, with or without consideration, may discharge the obligation of a party to pay the instrument (i) by an intentional voluntary act, such as surrender of the instrument to the party, destruction, mutilation, or cancellation of the instrument, cancellation or striking out of the party's signature, or the addition of words to the instrument indicating discharge, or (ii) by agreeing not to sue or otherwise renouncing rights against the party by a signed record. The obligation of a party to pay the instrument is not discharged solely by the destruction of a check in connection with a process in which, initially, information is extracted from the check and an image of the check is made and, subsequently, the information and image are transmitted for payment.

(b) Cancellation or striking out of an indorsement pursuant to subsection (a) does not affect the status and rights of a party derived from the indorsement.

(c) In this section, "signed," with respect to a record that is not a writing, includes the attachment to or logical association with the record of an electronic symbol, sound, or process with the present intent to adopt or accept the record.

Official Comment

Section 3–604 replaces former Section 3–605.

1. The destruction of a check in connection with a truncation process in which information is extracted from the check and an image of the check is made, and then such information and image are transmitted for payment is not within the scope of this section and does not by itself discharge the obligation of a party to pay the instrument. Such destruction also does not affect whether the check has been issued. See Section 3-105(a) and comment 1.

SECTION 4–207. TRANSFER WARRANTIES.

* * *

Official Comment

1. Except for subsection (b), this section conforms to Section 3–416 and extends its coverage to items. The substance of this section is discussed in the Comment to Section 3–416. Subsection (b) provides that customers or collecting banks that transfer items, whether by indorsement or not, undertake to pay the item if the item is dishonored. This obligation cannot be disclaimed by a "without recourse" indorsement or otherwise. With respect to checks, Regulation

CC Section 229.34 states the warranties made by paying and returning banks.

2. For an explanation of subsection (a)(6), see comment 8 to Section 3-416.

3. The warranties provided for in this Section, and in Sections 4-208 and 4-209 are supplemented by warranties created under federal law. For example, pursuant to Section 4-209(b), a person who undertakes to retain an item in connection with an agreement for electronic presentment makes a warranty that retention and presentment comply with the agreement. Under federal law, such a person might also make a warranty that no person will be asked to make payment based on a check already paid. See 12 C.F.R. § 229.34(a).

SECTION 4A–103. PAYMENT ORDER - DEFINITIONS.

(a) In this Article:

(1) "Payment order" means an instruction of a sender to a receiving bank, transmitted orally~~, electronically, or in writing~~ or in a record, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary if:

(i) the instruction does not state a condition to payment to the beneficiary other than time of payment,

(ii) the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender, and

(iii) the instruction is transmitted by the sender directly to the receiving bank or to an agent, funds-transfer system, or communication system for transmittal to the receiving bank.

* * *

Official Comment

This section is discussed in the Comment following Section 4A-104.

SECTION 4A–104. FUNDS TRANSFER - DEFINITIONS.

* * *

Official Comment

* * *

3. Further limitations on the scope of Article 4A are found in the three requirements found in subparagraphs (i), (ii), and (iii) of Section 4A-103(a)(1). Subparagraph (i) states that the instruction to pay is a payment order only if it "does not state a condition to payment to the beneficiary other than time of payment." An instruction to pay a beneficiary sometimes is subject to a requirement that the beneficiary perform some act such as delivery of documents.

~~For example,~~ **Example:** a New York bank may have issued a letter of credit in favor of X, a California seller of goods to be shipped to the New York bank's customer in New York. The terms of the letter of credit provide for payment to X if documents are presented to prove shipment of the goods. Instead of providing for presentment of the documents to the New York bank, the letter of credit states that they may be presented to a California bank that acts as an agent for payment. The New York bank sends an instruction to the California bank to pay X upon presentation of the required documents. The instruction is not covered by Article 4A because payment to the beneficiary is conditional upon receipt of shipping documents. The function of banks in a funds transfer under Article 4A is comparable to the role of banks in the collection and payment of checks in that it is essentially mechanical in nature. The low price and high speed that characterize funds transfers reflect this fact. Conditions to payment by the California bank other than time of payment impose responsibilities on that bank that go beyond those in Article 4A funds transfers. Although the payment by the New York bank to X under the letter of credit is not covered by Article 4A, if X is paid by the California bank, payment of the obligation of the New York bank to reimburse the California bank could be made by an Article 4A funds transfer. In such a case there is a distinction between the payment by the New York bank to X under the letter of credit and the payment by the New York bank to the California bank. For example, if the New York bank pays its reimbursement obligation to the California bank by a Fedwire naming the California bank as beneficiary (see Comment 1 to Section 4A-107), payment is made to the California bank rather than to X. That payment is governed by Article 4A and it could be made either before or after payment by the California bank to X. The payment by the New York bank to X under the letter of credit is not governed by Article 4A and it occurs when the California bank, as agent of the New York bank, pays X. No payment order was involved in that transaction. In this example, if the New York bank had erroneously sent an instruction to the California bank unconditionally instructing payment to X, the instruction would have been an Article 4A payment order. If the payment order was accepted (Section 4A-209(b)) by the California bank, a payment by the New York bank to X would have resulted (Section 4A-406(a)). But Article 4A would not prevent recovery of funds from X on the basis that X was not entitled to retain the funds under the law of mistake and restitution, letter of credit law or other applicable law.

An instruction to pay might be a component of a so-called "smart contract": a computer program or a transaction protocol intended to execute automatically. The fact that the smart contract itself is subject to a condition does not necessarily mean that an instruction to a payment issued pursuant to that smart contract "state[s] a condition to payment of the beneficiary" within the meaning of Section 4A-103(a)(1)(i). Whether the instruction does state such a condition depends on what the instruction says when it is received by the receiving bank. An instruction that neither grants discretion nor imposes a limitation on payment by the receiving bank does not state a condition to payment. What distinguishes the prior example is that the New York bank's instruction to the California bank did state a condition when the California bank received it.

Similarly, an instruction that is subject to a condition when received by Bank A, and which therefore does not constitute a payment order, does not become a payment order when the condition is satisfied. However, if, after the condition is satisfied, Bank A sends the instruction to Bank B without the stated condition, that second instruction could be a payment order if the instruction otherwise complies with Section 4A-103(a).

*** * ***

SECTION 4A–201. SECURITY PROCEDURE.

"Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may impose an obligation on the receiving bank or the customer and may require the use of algorithms or other codes, identifying words, ~~or~~ numbers, symbols, sounds or biometrics, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer or requiring that a payment order be sent from a known email address, IP address or phone number is not by itself a security procedure.

Official Comment

A large percentage of payment orders and communications amending or cancelling payment orders are transmitted electronically and it is standard practice to use security procedures that are designed to assure the authenticity of the message through steps designed to assure the identity of the sender, the integrity of the message, or both. Security procedures can also be used to detect error in the content of messages or to detect payment orders that are transmitted by mistake as in the case of multiple transmission of the same payment order. Security procedures might also apply to communications that are transmitted by telephone or in

~~writing~~ a record. Section 4A-201 defines these security procedures. The second sentence of the definition provides several examples of a security procedure, but this list is not exhaustive. The inclusion of the phrase "or similar security devices" means that, as new technologies emerge, what can be a security procedure will change. The definition of security procedure limits the term to a procedure "established by agreement of a customer and a receiving bank." The term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders. The question of whether loss that may result from the transmission of a spurious or erroneous payment order will be borne by the receiving bank or the sender or purported sender is affected by whether a security procedure was or was not in effect and whether there was or was not compliance with the procedure. Security procedures are referred to in Sections 4A-202 and 4A-203, which deal with authorized and verified payment orders, and Section 4A-205, which deals with erroneous payment orders.

Requiring that a payment order be sent from a known email, IP address or phone number is not by itself a "security procedure" within the meaning of this section because it is possible to make a payment order with a different origin appear to have been sent from such an address or phone number. However, requiring that a payment order have such an apparent origin in combination with other security protocols might be a security procedure.

SECTION 4A–202. AUTHORIZED AND VERIFIED PAYMENT ORDERS.

(a) A payment order received by the receiving bank is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency.

(b) If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the bank's obligations under the security procedure and any ~~written~~ agreement or instruction of the customer, evidenced by a record, restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates ~~a written~~ an agreement evidenced by a record with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.

(c) Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances

of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in ~~writing~~ a record to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the bank's obligations under the security procedure chosen by the customer.

* * *

Official Comment

This section is discussed in the Comment following Section 4A-203.

SECTION 4A–203. UNENFORCEABILITY OF CERTAIN VERIFIED PAYMENT ORDERS.

(a) If an accepted payment order is not, under Section 4A-202(a), an authorized order of a customer identified as sender, but is effective as an order of the customer pursuant to Section 4A-202(b), the following rules apply:

(1) By express ~~written~~ agreement evidenced by a record, the receiving bank may limit the extent to which it is entitled to enforce or retain payment of the payment order.

(2) The receiving bank is not entitled to enforce or retain payment of the payment order if the customer proves that the order was not caused, directly or indirectly, by a person (i) entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, or (ii) who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault. Information includes any access device, computer software, or the like.

(b) This section applies to amendments of payment orders to the same extent it applies to payment orders.

Official Comment

* * *

3. Subsection (b) of Section 4A-202 is based on the assumption that losses due to fraudulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged. The subsection is designed to protect both the customer and the receiving bank. A receiving bank needs to be able to rely on objective criteria to determine whether it can safely act on a payment order. Employees of the bank can be trained to "test" a payment order according to the various steps specified in the security procedure. The bank is responsible for the acts of these employees. Subsection (b)(ii) requires the bank to prove that it accepted the payment order in good faith and "in compliance with the bank's obligations under the security procedure." If the fraud was not detected because the bank's employee did not perform the acts required by the security procedure, the bank has not complied. Subsection (b)(ii) also requires the bank to prove that it complied with any agreement or instruction that restricts acceptance of payment orders issued in the name of the customer. If an agreement establishing a security procedure places obligations on both the sender and the receiving bank, the receiving bank need prove only that it complied with the obligations placed on the receiving bank. A customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank. For example, the customer may prohibit the bank from accepting a payment order that is not payable from an authorized account, that exceeds the credit balance in specified accounts of the customer, or that exceeds some other amount. Another limitation may relate to the beneficiary. The customer may provide the bank with a list of authorized beneficiaries and prohibit acceptance of any payment order to a beneficiary not appearing on the list. Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction. In either case, the bank must comply with the limitations if the conditions stated in subsection (b) are met. Normally limitations on acceptance would be incorporated into an agreement between the customer and the receiving bank, but in some cases the instruction might be unilaterally given by the customer. If standing instructions or an agreement state limitations on the ability of the receiving bank to act, provision must be made for later modification of the limitations. Normally this would be done by an agreement that specifies particular procedures to be followed. Thus, subsection (b) states that the receiving bank is not required to follow an instruction that violates ~~a written~~ an agreement evidenced by a record. The receiving bank is not bound by an instruction unless it has adequate notice of it. Subsections (25), (26) and (27) of Section 1-201 apply.

Subsection (b)(i) assures that the interests of the customer will be protected by providing an incentive to a bank to make available to the customer a security procedure that is commercially reasonable. If a commercially reasonable security procedure is not made available to the customer, subsection (b) does not apply. The result is that subsection (a) applies and the bank acts at its peril in accepting a payment order that may be unauthorized. Prudent banking practice may require that security procedures be utilized in virtually all cases except for those in

which personal contact between the customer and the bank eliminates the possibility of an unauthorized order. The burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud. The burden on the customer is to supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached.

4. The principal issue that is likely to arise in litigation involving subsection (b) is whether the security procedure in effect when a fraudulent payment order was accepted was commercially reasonable. In considering this issue, a court will need to consider the totality of the security procedure, including each party's obligations under such procedure. The concept of what is commercially reasonable in a given case is flexible. Verification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought. A customer that transmits very large numbers of payment orders in very large amounts may desire and may reasonably expect to be provided with state-of-the-art procedures that provide maximum security. But the expense involved may make use of a state-of-the-art procedure infeasible for a customer that normally transmits payment orders infrequently or in relatively low amounts. Another variable is the type of receiving bank. It is reasonable to require large money center banks to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank. A receiving bank might have several security procedures that are designed to meet the varying needs of different customers. The type of payment order is another variable. For example, in a wholesale wire transfer, each payment order is normally transmitted electronically and individually. A testing procedure will be individually applied to each payment order. In funds transfers to be made by means of an automated clearing house many payment orders are incorporated into an electronic device such as a magnetic tape that is physically delivered. Testing of the individual payment orders is not feasible. Thus, a different kind of security procedure must be adopted to take into account the different mode of transmission.

The issue of whether a particular security procedure is commercially reasonable is a question of law. Whether the receiving bank complied with the procedure is a question of fact. It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers. The purpose of subsection (b) is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. For example, the use of a computer program to detect fraud is not commercially unreasonable merely because it does not detect all fraud or because another system or approach might be more successful at detecting fraud. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. What is reasonable for a particular customer requires the court to consider the circumstances of the customer known to the bank, including the

size, type, and frequency of payment orders normally issued by the customer to the bank. Article 4A does not create an affirmative obligation on the receiving bank to obtain information about its customer. However, whatever knowledge the bank does have about the customer is relevant in determining the commercial reasonableness of the security procedure. ~~On the other hand, a~~ A security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank and customer should not be held to be commercially reasonable. Subsection (c) states factors to be considered by the judge in making the determination of commercial reasonableness. The reasonableness of a security procedure is to be determined at the time that a payment order is processed, not that the time the customer and the bank agree to the security procedure. Accordingly, a security procedure that was reasonable when agreed to might become unreasonable as technologies emerge, prevailing practices change, or the bank acquires knowledge about the customer. Sometimes an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper. In that case, under the last sentence of subsection (c), the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank. But this result follows only if the customer expressly agrees in ~~writing~~ a record to assume that risk. It is implicit in the last sentence of subsection (c) that a bank that accedes to the wishes of its customer in this regard is not acting in bad faith by so doing so long as the customer is made aware of the risk. In all cases, however, a receiving bank cannot get the benefit of subsection (b) unless it has made available to the customer a security procedure that is commercially reasonable and suitable for use by that customer. In most cases, the mutual interest of bank and customer to protect against fraud should lead to agreement to a security procedure which is commercially reasonable.

5. Subsection (b) generally allows a receiving bank to treat a payment order as authorized by the customer if the bank accepts the payment order in good faith and in compliance with the bank's obligations under a commercially reasonable, agreed-upon security procedure. For this purpose, "good faith" requires the exercise of reasonable commercial standards of fair dealing, *see* § 4A-105(a)(6), not the absence of negligence. Consequently, the bank has no duty, beyond that to which the bank has agreed, to investigate suspicious activity or to advise its customer of such activity. However, a bank that obtains knowledge that a customer's operations have been infiltrated or knowledge that the customer is the victim of identity fraud might not be acting in good faith if the bank, without receiving some assurance from the customer that the issue has been remediated, thereafter accepts a payment order.

~~5.~~6. The effect of Section 4A-202(b) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure. An exception to this result is provided by Section 4A-203(a)(2). The customer may avoid the loss resulting from such a payment order if the customer can prove that the fraud was not committed by a person described in that subsection. Breach of a commercially reasonable security procedure requires that the person committing the fraud have knowledge of how the procedure works and knowledge of codes, identifying devices, and the like. That person may also need access to transmitting facilities through an access device or other software in order to breach the security procedure. This confidential information must be obtained either from a source controlled by the customer

or from a source controlled by the receiving bank. If the customer can prove that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer or from a source controlled by the customer, the loss is shifted to the bank. "Prove" is defined in Section 4A-105(a)(7). Because of bank regulation requirements, in this kind of case there will always be a criminal investigation as well as an internal investigation of the bank to determine the probable explanation for the breach of security. Because a funds transfer fraud usually will involve a very large amount of money, both the criminal investigation and the internal investigation are likely to be thorough. In some cases there may be an investigation by bank examiners as well. Frequently, these investigations will develop evidence of who is at fault and the cause of the loss. The customer will have access to evidence developed in these investigations and that evidence can be used by the customer in meeting its burden of proof.

~~6.~~ 7. The effect of Section 4A-202(b) may also be changed by an agreement meeting the requirements of Section 4A-203(a)(1). Some customers may be unwilling to take all or part of the risk of loss with respect to unauthorized payment orders even if all of the requirements of Section 4A-202(b) are met. By virtue of Section 4A-203(a)(1), a receiving bank may assume all of the risk of loss with respect to unauthorized payment orders or the customer and bank may agree that losses from unauthorized payment orders are to be divided as provided in the agreement.

~~7.~~8. In a large majority of cases the sender of a payment order is a bank. In many cases in which there is a bank sender, both the sender and the receiving bank will be members of a funds transfer system over which the payment order is transmitted. Since Section 4A-202(f) does not prohibit a funds transfer system rule from varying rights and obligations under Section 4A-202, a rule of the funds transfer system can determine how loss due to an unauthorized payment order from a participating bank to another participating bank is to be allocated. A funds transfer system rule, however, cannot change the rights of a customer that is not a participating bank. § 4A-501(b). Section 4A-202(f) also prevents variation by agreement except to the extent stated.

SECTION 4A–206. TRANSMISSION OF PAYMENT ORDER THROUGH FUNDS-TRANSFER OR OTHER COMMUNICATION SYSTEM.

* * *

Official Comment

1. A payment order may be issued to a receiving bank directly by delivery of a ~~writing or electronic device~~ record or by an oral ~~or electronic~~ communication. If an agent of the sender is employed to transmit orders on behalf of the sender, the sender is bound by the order transmitted by the agent on the basis of agency law. Section 4A-206 is an application of that principle to cases in which a funds transfer or communication system acts as an intermediary in transmitting the sender's order to the receiving bank. The intermediary is deemed to be an agent of the sender for the purpose of transmitting payment orders and related messages for the sender. Section 4A-206 deals with error by the intermediary.

* * *

SECTION 4A–207. MISDESCRIPTION OF BENEFICIARY.

* * *

(c) If (i) a payment order described in subsection (b) is accepted, (ii) the originator's payment order described the beneficiary inconsistently by name and number, and (iii) the beneficiary's bank pays the person identified by number as permitted by subsection (b)(1), the following rules apply:

(1) If the originator is a bank, the originator is obliged to pay its order.

(2) If the originator is not a bank and proves that the person identified by number was not entitled to receive payment from the originator, the originator is not obliged to pay its order unless the originator's bank proves that the originator, before acceptance of the originator's order, had notice that payment of a payment order issued by the originator might be made by the beneficiary's bank on the basis of an identifying or bank account number even if it identifies a person different from the named beneficiary. Proof of notice may be made by any admissible evidence. The originator's bank satisfies the burden of proof if it proves that the originator, before the payment order was accepted, ~~signed a writing~~ authenticated a record stating the information to which the notice relates.

*** * ***

SECTION 4A–208. MISDESCRIPTION OF INTERMEDIARY BANK OR BENEFICIARY'S BANK.

* * *

(b) * * *

(2) If the sender is not a bank and the receiving bank proves that the sender, before the payment order was accepted, had notice that the receiving bank might rely on the number as the proper identification of the intermediary or beneficiary's bank even if it identifies a person different from the bank identified by name, the rights and obligations of the sender and the receiving bank are governed by subsection (b)(1), as though the sender were a bank. Proof of notice may be made by any admissible evidence. The receiving bank satisfies the burden of proof if it proves that the sender, before the payment order was accepted, ~~signed a writing~~ authenticated a record stating the information to which the notice relates.

* * *

SECTION 4A–210. REJECTION OF PAYMENT ORDER.

(a) A payment order is rejected by the receiving bank by a notice of rejection transmitted to the sender orally~~, electronically,~~ or in ~~writing~~ a record. A notice of rejection need not use any particular words and is sufficient if it indicates that the receiving bank is rejecting the order or will not execute or pay the order. Rejection is effective when the notice is given if transmission is by a means that is reasonable in the circumstances. If notice of rejection is given by a means that is not reasonable, rejection is effective when the notice is received. If an agreement of the sender and receiving bank establishes the means to be used to reject a payment order, (i) any means complying with the agreement is reasonable and (ii) any means not complying is not reasonable unless no significant delay in receipt of the notice resulted from the use of the noncomplying means.

* * *

SECTION 4A–211. CANCELLATION AND AMENDMENT OF PAYMENT ORDER.

(a) A communication of the sender of a payment order cancelling or amending the order may be transmitted to the receiving bank orally~~, electronically,~~ or in ~~writing~~ a record. If a

security procedure is in effect between the sender and the receiving bank, the communication is not effective to cancel or amend the order unless the communication is verified pursuant to the security procedure or the bank agrees to the cancellation or amendment.

* * *

.

Official Comment

* * *

2. Subsection (a) allows a cancellation or amendment of a payment order to be communicated to the receiving bank "orally~~, electronically,~~ or in ~~writing~~ a record." The quoted phrase is consistent with the language of Section 4A-103(a) applicable to payment orders. Cancellations and amendments are normally subject to verification pursuant to security procedures to the same extent as payment orders. Subsection (a) recognizes this fact by providing that in cases in which there is a security procedure in effect between the sender and the receiving bank the bank is not bound by a communication cancelling or amending an order unless verification has been made. This is necessary to protect the bank because under subsection (b) a cancellation or amendment can be effective by unilateral action of the sender. Without verification the bank cannot be sure whether the communication was or was not effective to cancel or amend a previously verified payment order.